

# Identificatie en beperking van benutting van de kwetsbaarheid van Cisco IOS-software release Data-Link-switching

# Identificatie en beperking van benutting van de kwetsbaarheid van Cisco IOS-software release Data-Link-switching

Advies-ID: cisco-amb-20110928-dlsw

<https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20110928-dlsw>

## Revisie 1.0

Voor Openbare Publicatie 2011 September 28 16:00 UTC (GMT)

---

## Inhoud

[Cisco Response](#)

[Apparaatspecifieke beperking en identificatie](#)

[Aanvullende informatie](#)

[Revisiegeschiedenis](#)

[Cisco-beveiligingsprocedures](#)

[Gerelateerde informatie](#)

---

## Cisco Response

Dit Toegepaste Mitigation Bulletin is een begeleidend document bij de PSIRT Security Advisory *Cisco IOS-software voor datalink-switching* kwetsbaarheid en biedt identificatie- en mitigatietechnieken die beheerders op Cisco-netwerkapparaten kunnen implementeren.

## Kwetsbaarheid Kenmerken

Cisco IOS-software bevat een kwetsbaarheid bij het verwerken van misvormde DLSw-pakketten (Data-Link Switching). Deze kwetsbaarheid kan op afstand worden benut zonder authenticatie en zonder interactie van de eindgebruiker. Succesvolle benutting van deze kwetsbaarheid kan resulteren in een denial of service-omstandigheid (DoS). Herhaalde pogingen om gebruik te maken van deze kwetsbaarheid kunnen resulteren in een aanhoudende DoS-conditie. De aanvalsvector voor exploitatie is via IP-protocol 91-pakketten. Een aanvaller kon deze kwetsbaarheid exploiteren met spoofed pakketten.

Deze kwetsbaarheid is toegewezen CVE-identificatiecode CVE-2011-0945.

## Overzicht van kwetsbaarheden

Informatie over kwetsbare, onaangetaste en vaste software is beschikbaar in de PSIRT Security Advisory, die beschikbaar is via de volgende link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw>.

## Overzicht Mitigation Technique

Cisco-apparaten bieden verschillende tegenmaatregelen voor deze kwetsbaarheid. Beheerders wordt aangeraden deze beveiligingsmethoden te beschouwen als algemene best practices op het gebied van beveiliging van infrastructuurapparaten en het verkeer dat het netwerk doorkruist. In dit gedeelte van het document wordt een overzicht van deze technieken gegeven.

Cisco IOS-software kan effectieve middelen voor explosiepreventie bieden door gebruik te maken van de volgende methoden:

- Toegangscontrolelijsten voor infrastructuur (iACL's)
- Unicast Reverse Path Forwarding (Unicast RPF)
- IP-bronbeveiliging (IPSG)

Deze beschermingsmechanismen filteren en laten vallen, en verifiëren het IP-adres van de bron van pakketten die deze kwetsbaarheid proberen te exploiteren.

De juiste implementatie en configuratie van Unicast RPF biedt een effectieve bescherming tegen aanvallen die pakketten met IP-adressen van gespoofde bronnen gebruiken. Unicast RPF moet zo dicht mogelijk bij alle verkeersbronnen worden geïmplementeerd.

De juiste plaatsing en configuratie van IPSG biedt een effectief middel tegen spoofingaanvallen op de toegangslaag.

Effectieve middelen voor explosiepreventie kunnen ook worden geleverd door de Cisco ASA 5500 Series adaptieve security applicatie en de Firewall Services Module (FWSM) voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers met de volgende methoden:

- Toegangscontrolelijsten voor douanevervoer (ACL's)
- Unicast RPF

Deze beschermingsmechanismen filteren en laten vallen, en verifiëren het IP-adres van de bron van pakketten die deze kwetsbaarheid proberen te exploiteren.

Cisco IOS NetFlow-records kunnen zichtbaarheid bieden in netwerkgebaseerde exploitatiepogingen.

Cisco IOS-software, Cisco ASA en Cisco FWSM-firewalls kunnen zichtbaarheid bieden door syslog-berichten en tegenwaarden die worden weergegeven in de uitvoer van **show**-opdrachten.

## Risicobeheer

Organisaties wordt aangeraden hun standaardprocessen voor risicobeoordeling en risicobeperking te volgen om de mogelijke gevolgen van deze kwetsbaarheid te bepalen. Triage

verwijst naar het sorteren van projecten en het prioriteren van inspanningen die waarschijnlijk het meest succesvol zullen zijn. Cisco heeft documenten geleverd die organisaties kunnen helpen bij de ontwikkeling van een op risico gebaseerde triagecapaciteit voor hun informatieveiligheidsteams. [Risico Triage voor Security Vulnerability aankondigingen](#) en [Risk Triage en Prototyping](#) kunnen organisaties helpen herhaalbare security evaluatie- en reactieprocessen te ontwikkelen.

## Apparaatspecifieke beperking en identificatie

**Waarschuwing:** de effectiviteit van elke mitigatietechniek hangt af van specifieke klantsituaties, zoals productmix, netwerktopologie, verkeersgedrag en organisatorische missie. Zoals bij elke configuratiewijziging, evalueer het effect van deze configuratie voordat u de wijziging toepast.

Voor deze hulpmiddelen is specifieke informatie over beperking en identificatie beschikbaar:

- [Cisco IOS-routers en -Switches](#)
- [Cisco IOS NetFlow](#)
- [Cisco ASA- en FWSM-firewalls](#)

### [Cisco IOS-routers en -Switches](#)

#### **Beperking: toegangscontrolelijsten voor infrastructuur**

Om infrastructuurapparaten te beschermen en het risico, de impact en de effectiviteit van directe infrastructuuraanvallen te minimaliseren, wordt beheerders aangeraden om lijsten met toegangscontroles voor de infrastructuur (iACL's) te implementeren om beleidshandhaving uit te voeren van verkeer dat naar infrastructuurapparatuur wordt verzonden. Beheerders kunnen een iACL construeren door alleen geautoriseerd verkeer toe te staan dat naar infrastructuurapparaten wordt verzonden in overeenstemming met bestaand beveiligingsbeleid en configuraties. Voor een maximale bescherming van infrastructurele apparaten moeten gebruikte iACL's worden toegepast in de toegangsrichting op alle interfaces waarvoor een IP-adres is geconfigureerd. Een iACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheid bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het iACL-beleid ontkent onbevoegde DLSw-pakketten op IP-protocol 91 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend. Waar mogelijk moet de adresruimte van de infrastructuur worden onderscheiden van de adresruimte die wordt gebruikt voor gebruikers- en dienstensegmenten. Het gebruik van deze adresseringsmethodologie zal helpen bij de constructie en implementatie van iACL's.

Aanvullende informatie over iACL's is te vinden in [Protected Your Core: Infrastructure Protection Access Control Lists](#).

```
ip access-list extended Infrastructure-ACL-Policy
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable protocol
```

```

!
permit 91 host 192.168.100.1 192.168.60.0 0.0.0.255
!
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
!
deny 91 any 192.168.60.0 0.0.0.255
!
!-- Explicit deny ACE for traffic sent to addresses configured within
!-- the infrastructure address space
!
deny ip any 192.168.60.0 0.0.0.255
!
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Apply iACL to interfaces in the ingress direction
!
interface GigabitEthernet0/0
ip access-group Infrastructure-ACL-Policy in

```

Merk op dat het filteren met een lijst van de interfacetoegang de transmissie van onbereikbare berichten ICMP terug naar de bron van het gefilterde verkeer zal veroorzaken. Het genereren van deze berichten zou het ongewenste effect kunnen hebben van het verhogen van CPU-gebruik op het apparaat. In Cisco IOS-software is de onbereikbare ICMP-generatie standaard beperkt tot één pakket per 500 milliseconden. ICMP onbereikbare berichtgeneratie kan worden uitgeschakeld met de opdracht interfaceconfiguratie **zonder IP-onbereikbaar**. ICMP-onbereikbare snelheidsbeperking kan worden gewijzigd ten opzichte van de standaardinstelling met behulp van de **algemene** opdracht voor configuratie **ip icmp-snelheidslimiet voor onbereikbare interval-in-ms**.

## Beperken: bescherming tegen spoofing

### Unicast doorsturen van omgekeerde paden

De kwetsbaarheid die in dit document wordt beschreven, kan worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast Reverse Path Forwarding (Unicast RPF) implementeren en configureren als een beschermingsmechanisme tegen spoofing.

Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. Beheerders wordt aangeraden ervoor te zorgen dat de juiste Unicast RPF-modus (los of strikt) wordt geconfigureerd tijdens de implementatie van deze functie, omdat legitiem verkeer dat het netwerk oversteeft kan worden geminimaliseerd. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.

Aanvullende informatie vindt u in de [Unicast Reverse Path Forwarding Loose Mode functiehandleiding](#).

Voor extra informatie over de configuratie en het gebruik van Unicast RPF, raadpleegt u het Witboek [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence.

## IP-bronbeveiliging

IP Source Guard (IPSG) is een beveiligingsfunctie die IP-verkeer op niet-gerouteerde, Layer 2-interfaces beperkt door pakketten te filteren op basis van de bindende database met DHCP-snooping en handmatig ingestelde IP-bronbindingen. Beheerders kunnen IPSG gebruiken om aanvallen te voorkomen van een aanvaller die probeert pakketten te parasiteren door het IP-bronadres en/of het MAC-adres te vervalsen. Wanneer correct geïmplementeerd en geconfigureerd, biedt IPSG in combinatie met de strikte modus Unicast RPF de meest effectieve bescherming tegen spoofing voor de kwetsbaarheid die in dit document wordt beschreven.

Aanvullende informatie over de implementatie en configuratie van IPSG is te vinden in [Configureren DHCP-functies en IP Source Guard](#).

### Identificatie: Toegangscontrolelijsten voor infrastructuur

Nadat de beheerder iACL op een interface heeft toegepast, zal de opdracht **IP-toeganglijsten tonen** het aantal DLSw-pakketten op IP-protocol 91 identificeren dat is gefilterd op interfaces waarop iACL is toegepast. De beheerders zouden gefilterde pakketten moeten onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont ip toegang-lijsten Infrastructuur-ACL-Beleid** volgt:

```
router#show ip access-lists Infrastructure-ACL-Policy
Extended IP access list Infrastructure-ACL-Policy
10 permit 91 host 192.168.100.1 192.168.60.0 0.0.0.255
20 deny 91 any 192.168.60.0 0.0.0.255 (8 matches)
30 deny ip any 192.168.60.0 0.0.0.255
router#
```

In het bovenstaande voorbeeld is de *infrastructuur-ACL-beleid* in de toeganglijst gedaald met **8 DLSw-pakketten** op **IP-protocol 91** voor regel 20 van de toegangscontrolelijst.

Voor extra informatie over het onderzoeken van incidenten met ACE-tellers en syslog-gebeurtenissen, raadpleegt u het white paper [Identifying Incidents Use Firewall en IOS Router Syslog Events](#) Applied Intelligence.

Beheerders kunnen Embedded Event Manager gebruiken om instrumentatie te bieden wanneer aan specifieke voorwaarden is voldaan, zoals ACE-tellers. De Applied Intelligence white paper [Embedded Event Manager in een security context](#) biedt aanvullende informatie over hoe deze functie te gebruiken.

### Identificatie: Vastlegging toeganglijst

De optie **log** en **log-input** toegangcontrolelijst (ACL) zorgt ervoor dat pakketten die overeenkomen met specifieke ACE's worden vastgelegd. De **log-input**optie maakt het registreren van de toegangsinterface mogelijk, naast de IP-adressen en -poorten van de pakketbron en de bestemming.

**Waarschuwing:** vastlegging in toegangcontrolelijst kan zeer CPU-intensief zijn en moet met uiterste voorzichtigheid worden gebruikt. De factoren die de CPU-impact van ACL-vastlegging bepalen, zijn loggeneratie, logtransmissie en processwitching naar voorwaartse pakketten die logbestanden met ACE's matchen.

Voor Cisco IOS-software kan de opdracht **interval-in-ms vastlegging van IP-toeganglijst** de effecten van processwitching beperken die worden geïnduceerd door ACL-vastlegging. De **logsnelheid-limiet** *rate-per-seconde* [**behalve loglevel**] opdracht beperkt het effect van loggeneratie en transmissie.

De CPU-impact van ACL-vastlegging kan worden aangepakt in hardware op de Cisco Catalyst 6500 Series-switches en Cisco 7600 Series-routers met Supervisor Engine 720 of Supervisor Engine 32 met behulp van geoptimaliseerde ACL-vastlegging.

Voor extra informatie over de configuratie en het gebruik van ACL-vastlegging raadpleegt u het Witboek [Inzicht in toegangscontrolelijst](#) en toegepaste intelligentie.

## Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding

Met Unicast RPF correct geïmplementeerd en geconfigureerd in de netwerkinfrastructuur, kunnen beheerders de *sleuf/poort* van het *type show cef interfacetype intern* gebruiken, **ip-interface tonen**, **cef-drop tonen**, **ip cef-switching statistieken-functie tonen**, en **ip traffic** opdrachten tonen om het aantal pakketten te identificeren dat Unicast RPF is gedaald.

**Opmerking:** beginnend met Cisco IOS-software release 12.4(20)T is de opdracht **ip cef-switching** vervangen door de **functie IP cef-switching**.

**Opmerking:** de *opdracht show | begin met regex en toon opdracht | regex-opdrachtwijzigingen omvatten* die in de volgende voorbeelden worden gebruikt om de hoeveelheid output te minimaliseren die beheerders moeten parseren om de gewenste informatie te bekijken. Er is aanvullende informatie over opdrachtbepalingen in de secties [met](#) de [opdracht show](#) van de opdrachtreferentie voor Cisco IOS Configuration Fundamentals.

```
router#show cef interface GigabitEthernet 0/0 internal | include drop
ip verify: via=rx (allow default), acl=0, drop=7, sdrop=0
router#
```

**Opmerking:** **tonen cef interface type sleuf / poort intern** is een verborgen opdracht die volledig moet worden ingevoerd op de opdrachtregel interface. Opdrachtvoltooiing is er niet voor beschikbaar.

```
router#show ip interface GigabitEthernet 0/0 | begin verify
IP verify source reachable-via RX, allow default, allow self-ping 7 verification
drops
  0 suppressed verification drops
router#
```

```
router#show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved  Unsupported  No_route  No_adj  ChkSum_Err
RP      27            0            0            7         0       0
router#
```

```
router#show ip cef switching statistics feature
```

```
IPv4 CEF input features:
Path Feature Drop    Consume    Punt  Punt2Host  Gave route
RP PAS uRPF      7         0        0        0        0
Total 7 0 0 0 0 -- CLI Output Truncated -- router# router#show ip traffic | include
RPF
```

```
7 no route, 7 unicast RPF, 0 forced drop
```

```
router#
```

In de voorgaande **show cef drop**, **toon ip cef switching statistieken functie**, en **toon ip traffic** voorbeelden, Unicast RPF heeft laten vallen **7 IP pakketten** die globaal ontvangen op alle

interfaces met Unicast RPF geconfigureerd vanwege het onvermogen om het bronadres van de IP pakketten te verifiëren binnen de Forwarding Information Base van Cisco Express Forwarding.

## Cisco IOS NetFlow

### Identificatie: Traffic Flow Identification met NetFlow-records

Beheerders kunnen Cisco IOS NetFlow configureren op Cisco IOS-routers en -switches om te helpen bij de identificatie van verkeersstromen die pogingen kunnen zijn om de kwetsbaarheid te exploiteren. De beheerders worden geadviseerd om stromen te onderzoeken om te bepalen of zij pogingen zijn om de kwetsbaarheid te exploiteren of of zij wettige verkeersstromen zijn.

```
router#show ip cache flow
```

```
IP packet size distribution (90784136 total packets):
```

```
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .698 .011 .001 .004 .005 .000 .004 .000 .000 .003 .000 .000 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .001 .256 .000 .010 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 4456704 bytes
```

```
1885 active, 63651 inactive, 59960004 added
129803821 aged polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
```

```
IP Sub Flow Cache, 402056 bytes
```

```
0 active, 16384 inactive, 0 added, 0 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics never
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Flow)	Idle(Flow)
TCP-Telnet	11393421	2.8	1	48	3.1	0.0	1.4
TCP-FTP	236	0.0	12	66	0.0	1.8	4.8
TCP-FTPD	21	0.0	13726	1294	0.0	18.4	4.1
TCP-WWW	22282	0.0	21	1020	0.1	4.1	7.3
TCP-X	719	0.0	1	40	0.0	0.0	1.3
TCP-BGP	1	0.0	1	40	0.0	0.0	15.0
TCP-Frag	70399	0.0	1	688	0.0	0.0	22.7
TCP-other	47861004	11.8	1	211	18.9	0.0	1.3
UDP-DNS	582	0.0	4	73	0.0	3.4	15.4
UDP-NTP	287252	0.0	1	76	0.0	0.0	15.5
UDP-other	310347	0.0	2	230	0.1	0.6	15.9
ICMP	11674	0.0	3	61	0.0	19.8	15.5
IPv6INIP	15	0.0	1	1132	0.0	0.0	15.4
GRE	4	0.0	1	48	0.0	0.0	15.3
Total:	59957957	14.8	1	196	22.5	0.0	1.5

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
<b>Gi0/0</b>	<b>192.168.10.201</b>	<b>Gi0/1</b>	<b>192.168.60.102</b>	<b>5B</b>	<b>0000</b>	<b>0000</b>	<b>11</b>
<b>Gi0/0</b>	<b>192.168.11.54</b>	<b>Gi0/1</b>	<b>192.168.60.158</b>	<b>5B</b>	<b>0000</b>	<b>0000</b>	<b>8</b>
Gi0/1	192.168.150.60	Gi0/0	10.89.16.226	06	0016	12CA	1
<b>Gi0/0</b>	<b>192.168.10.17</b>	<b>Gi0/1</b>	<b>192.168.60.97</b>	<b>5B</b>	<b>0000</b>	<b>0000</b>	<b>2</b>
Gi0/0	10.88.226.1	Gi0/1	192.168.202.22	11	007B	007B	1
Gi0/0	10.89.16.226	Gi0/1	192.168.150.60	06	12CA	0016	1

```
router#
```

In het bovenstaande voorbeeld zijn er meerdere stromen voor **DLSw** op **IP-protocol 91**

(hexuitdraai waarde 5B).

Dit verkeer wordt verzonden naar adressen binnen het 192.168.60.0/24 adresblok, dat door getroffen apparaten wordt gebruikt. De pakketten in deze stromen kunnen worden gespoofd en kunnen wijzen op een poging om deze kwetsbaarheid te exploiteren. De beheerders worden geadviseerd om deze stromen bij basislijngebruik voor verkeer te vergelijken DLSw dat op IP protocol 91 wordt verzonden en ook de stromen te onderzoeken om te bepalen of zij van onbetrouwbare gastheren of netwerken afkomstig zijn.

Als u alleen de verkeersstromen voor DLSw-pakketten op IP-protocol 91 (hexadecimale waarde 5B) wilt weergeven, **toont** de opdracht de **IP-cachestroom | neem SrcIf\_5B\_** zal de verwante IP-protocol 91 NetFlow records zoals hier getoond tonen:

```
router#show ip cache flow | include SrcIf|_5B_
SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr SrcP DstP  Pkts
Gi0/0 192.168.12.110 Gi0/1 192.168.60.163 5B 0000 0000 11
Gi0/0 192.168.11.230 Gi0/1 192.168.60.20 5B 0000 0000 13
Gi0/0 192.168.11.131 Gi0/1 192.168.60.245 5B 0000 0000 7
router#
```

## [Cisco ASA- en FWSM-firewalls](#)

### Beperking: toegangscontrolelijsten voor douanevervoer

Om het netwerk te beschermen tegen verkeer dat het netwerk ingaat op toegangspunten die internetverbindingpunten, partner- en leverancierverbindingen of VPN-verbindingpunten kunnen omvatten, wordt beheerders aangeraden om tACL's te implementeren om beleidshandhaving uit te voeren. Beheerders kunnen een tACL construeren door alleen geautoriseerd verkeer expliciet toe te staan om het netwerk op access points binnen te gaan of door geautoriseerd verkeer toe te staan om door het netwerk te reizen in overeenstemming met bestaand beveiligingsbeleid en configuraties. Een tACL-tijdelijke oplossing kan geen volledige bescherming tegen deze kwetsbaarheid bieden wanneer de aanval afkomstig is van een vertrouwd bronadres.

Het tACL-beleid ontkent onbevoegde DLSw-pakketten op IP-protocol 91 die naar getroffen apparaten worden verzonden. In het volgende voorbeeld, 192.168.60.0/24 is de IP adresruimte die door de beïnvloede apparaten wordt gebruikt, en de gastheer in 192.168.100.1 wordt beschouwd als een vertrouwde op bron die toegang tot de beïnvloede apparaten vereist. Zorg ervoor dat het vereiste verkeer voor routing en administratieve toegang is toegestaan voordat alle niet-geautoriseerde verkeer wordt ontkend.

Aanvullende informatie over tACL's staat in [Transit Access Control Lists: Filtering at Your Edge](#).

```
!
!-- Include explicit permit statements for trusted sources
!-- that require access on the vulnerable protocol
! access-list tACL-Policy extended permit 91 host 192.168.100.1 192.168.60.0
255.255.255.0 !
!-- The following vulnerability-specific access control entry
!-- (ACE) can aid in identification of attacks
! access-list tACL-Policy extended deny 91 any 192.168.60.0 255.255.255.0 !
!-- Permit or deny all other Layer 3 and Layer 4 traffic in accordance
!-- with existing security policies and configurations
!
!-- Explicit deny for all other IP traffic
! access-list tACL-Policy extended deny ip any any !
```



```
!-- Apply tACL to interface(s) in the ingress direction
! access-group tACL-Policy in interface outside
```

## Beperking: bescherming tegen spoofing met Unicast Reverse Path Forwarding

De kwetsbaarheid die in dit document wordt beschreven, kan worden benut door gespoofde IP-pakketten. Beheerders kunnen Unicast RPF implementeren en configureren als een beschermingsmechanisme tegen spoofing.

Unicast RPF is geconfigureerd op interfaceniveau en kan pakketten detecteren en neerzetten die geen verifieerbaar IP-bronadres hebben. Beheerders dienen niet te vertrouwen op Unicast RPF om volledige bescherming tegen spoofing te bieden, omdat spoofed-pakketten het netwerk via een Unicast RPF-enabled interface kunnen binnenkomen als er een geschikte retourroute naar het bron-IP-adres bestaat. In een ondernemingsmilieu, zou Unicast RPF bij de rand van Internet en bij de interne toegangslaag op gebruiker-ondersteunende Layer 3 kunnen worden toegelaten interfaces.

Voor extra informatie over de configuratie en het gebruik van Unicast RPF, raadpleegt u de Cisco Security Appliance Command Reference voor [IP-verificatie van het omgekeerde pad](#) en het [Understanding Unicast Reverse Path Forwarding](#) Applied Intelligence-witboek.

## Identificatie: Toegangscontrolelijsten voor douanevervoer

Nadat tACL is toegepast op een interface, kunnen beheerders de **show access-list** opdracht gebruiken om het aantal DLSw-pakketten op IP-protocol 91 te identificeren die zijn gefilterd. De beheerders worden geadviseerd om gefilterde pakketten te onderzoeken om te bepalen of zij pogingen zijn om deze kwetsbaarheid te exploiteren. De output van het voorbeeld voor **toont toegang-lijst aan ACL-Beleid** volgt:

```
firewall#show access-list tACL-Policy
access-list tACL-Policy; 3 elements
access-list tACL-Policy line 1 extended permit 91 host 192.168.100.1
    192.168.60.0 255.255.255.0 (hitcnt=34)
access-list tACL-Policy line 2 extended deny 91 any
    192.168.60.0 255.255.255.0 (hitcnt=6)
access-list tACL-Policy line 3 extended deny ip any any (hitcnt=8)
firewall#
```

In het voorafgaande voorbeeld, heeft de toegangslijst *van ACL-Beleid 6* DLSw-pakketten op **IP-protocol 91** laten vallen die van een onbetrouwbare host of een onbetrouwbaar netwerk zijn ontvangen. Daarnaast kan syslog-bericht *106023* waardevolle informatie leveren, waaronder het IP-adres van de bron en de bestemming, de bron- en doelpoortnummers en het IP-protocol voor het ontkende pakket.

## Identificatie: berichten in Firewall Access List System

Firewallsyslog-bericht *106023* wordt gegenereerd voor pakketten die worden geweigerd door een toegangscontrole-ingang (ACE) die niet het trefwoord voor het **logbestand** heeft. Aanvullende informatie over dit syslogbericht wordt weergegeven in [Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106023](#).

Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie is beschikbaar in [Monitoring - Configuration Logging](#). De informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600

Series routers is beschikbaar in [Monitoring the Firewall Services Module](#).

In het volgende voorbeeld, de **show vastlegging | grep regex** opdracht haalt syslog berichten uit de logboekbuffer op de firewall. Deze berichten verstrekken extra informatie over ontkende pakketten die op potentiële pogingen zouden kunnen wijzen om de kwetsbaarheid te exploiteren die in dit document wordt beschreven. Het is mogelijk om verschillende reguliere expressies te gebruiken met het **grep**-sleutelwoord om te zoeken naar specifieke gegevens in de geregistreerde berichten.

Aanvullende informatie over de syntaxis van reguliere expressies is te vinden in [Create a Regular Expression](#).

```
firewall#show logging | grep 106023
```

```
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.18
dst inside:192.168.60.191 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.200
dst inside:192.168.60.33 by access-group "tACL-Policy"
Sep 28 2011 01:10:31: %ASA-4-106023: Deny protocol 91 src outside:192.0.2.99
dst inside:192.168.60.240 by access-group "tACL-Policy"
```

```
firewall#
```

In het voorafgaande voorbeeld, tonen de berichten die voor tACL *tACL-Policy* zijn geregistreerd potentieel gespoofde **DLSw**-pakketten voor **IP-protocol 91** die naar het adresblok zijn verzonden dat aan de betreffende apparaten is toegewezen.

Aanvullende informatie over syslogberichten voor ASA-beveiligingsapparaten is te vinden in [Cisco ASA 5500 Series systeemlogberichten, 8.2](#). Aanvullende informatie over syslog-berichten voor de FWSM is te vinden in [Catalyst 6500 Series Switch en Cisco 7600 Series router Firewall Services Module Logging System Berichten](#).

Voor extra informatie over het onderzoeken van incidenten met behulp van syslog-gebeurtenissen, raadpleegt u het white paper [Identifying Incidents Using Firewall en IOS Router Syslog Events](#) Applied Intelligence.

## Identificatie: bescherming tegen spoofing met Unicast Reverse Path Forwarding

Firewallsyslog-bericht *106021* wordt gegenereerd voor pakketten die worden geweigerd door Unicast PDF. Aanvullende informatie over dit syslogbericht wordt weergegeven in [Cisco ASA 5500 Series systeemlogbericht, 8.2 - 106021](#).

Informatie over het configureren van syslog voor de Cisco ASA 5500 Series adaptieve security applicatie is beschikbaar in [Monitoring - Configuration Logging](#). De informatie over het configureren van syslog op de FWSM voor Cisco Catalyst 6500 Series switches en Cisco 7600 Series routers is beschikbaar in [Monitoring the Firewall Services Module](#).

In het volgende voorbeeld, de **show vastlegging | grep regex** opdracht haalt syslog berichten uit de logboekbuffer op de firewall. Deze berichten verstrekken extra informatie over ontkende pakketten die op potentiële pogingen zouden kunnen wijzen om de kwetsbaarheid te exploiteren die in dit document wordt beschreven. Het is mogelijk om verschillende reguliere expressies te gebruiken met het **grep**-sleutelwoord om te zoeken naar specifieke gegevens in de geregistreerde berichten.

Aanvullende informatie over de syntaxis van reguliere expressies is te vinden in [Create a Regular Expression](#).

```
firewall#show logging | grep 106021
```

```
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from  
192.168.60.1 to 192.168.60.191 on interface outside  
Sep 28 2011 02:00:23: %ASA-1-106021: Deny protocol 91 reverse path check from  
192.168.60.1 to 192.168.60.33 on interface outside
```

De opdracht **Snel** starten tonen kan ook het aantal pakketten identificeren dat de Unicast RPF-functie is gevallen, zoals in het volgende voorbeeld:

```
firewall#show asp drop frame rpf-violated  
Reverse-path verify failed 16  
firewall#
```

In het voorafgaande voorbeeld, Unicast RPF **16 pakketten** gedaald die op interfaces met Unicast RPF worden ontvangen gevormd. Het ontbreken van uitvoer geeft aan dat de Unicast RPF-functie op de firewall geen pakketten heeft laten vallen.

Voor extra informatie over het debuggen van versnelde security pad gedropte pakketten of verbindingen, verwijzen we naar de Cisco Security Appliance Command Reference voor [show asp drop](#).

## Aanvullende informatie

DIT DOCUMENT WORDT AANGEBODEN OP EEN 'AS IS'-BASIS EN IMPLICEERT GEEN ENKEL SOORT GARANTIE, MET INBEGRIJ VAN GARANTIES VAN VERKOOPBAARHEID OF GESCHIKTHEID VOOR EEN BEPAALD DOEL. UW GEBRUIK VAN DE INFORMATIE IN HET DOCUMENT OF DE MATERIALEN GEKOPPELD AAN HET DOCUMENT IS GEHEEL OP EIGEN RISICO. CISCO BEHOUDT ZICH HET RECHT VOOR OM DIT DOCUMENT TE ALLEN TIJDE TE WIJZIGEN OF TE ANNULEREN.

## Revisiegeschiedenis

Revisie 1.0	2011-28 SEPTEMBER	Eerste openbare publicatie
-------------	-------------------	----------------------------

## Cisco-beveiligingsprocedures

Volledige informatie over het melden van beveiligingskwetsbaarheden in Cisco-producten, het verkrijgen van assistentie bij beveiligingsincidenten en het registreren om beveiligingsinformatie van Cisco te ontvangen, is beschikbaar op de wereldwijde website van Cisco op [https://sec.cloudapps.cisco.com/security/center/resources/security\\_vulnerability\\_policy.html](https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html). Dit omvat instructies voor persvragen over Cisco-beveiligingsmeldingen. Alle Cisco-beveiligingsadviezen zijn beschikbaar op <http://www.cisco.com/go/psirt>.

## Gerelateerde informatie

- [Cisco-bulletins voor toegepaste beperking](#)
- [Cisco-beveiligingsintelligentie](#)
- [Cisco Security IntelliShield Alert Manager-service](#)
- [Cisco-handleiding over het versterken van Cisco IOS-apparaten](#)
- [Cisco IOS NetFlow - startpagina op Cisco.com](#)

- [Cisco IOS NetFlow-witboeken](#)
- [NetFlow-prestatieanalyse](#)
- [Witboeken voor Cisco Network Foundation-bescherming](#)
- [Presentaties voor Cisco Network Foundation-bescherming](#)
- [Een security georiënteerde benadering van IP-adressering](#)
- [Cisco Firewallproducten - startpagina op Cisco.com](#)
- [Verbeteringen in Unicast Reverse Path Forwarding voor de Internet Service Provider](#)
- [Gemeenschappelijke kwetsbaarheden en blootstellingen \(CVE\)](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.